SECURITY DISCUSSION

George A. White

Technical Architecture Group

FBI/CJIS Division

OVERVIEW

- **Directives**

- **Potentials**

- **Relevance**

- **Discussion**

Directives

- **OMB Memorandum, Protection Of Sensitive Agency Information, June 23, 2006…**
  - Allow Remote Access Only With Two-factor Authentication Where One Of The Factors Is Provided By A Device Separate From The Computer Gaining Access.

- **Deputy Attorney General Memorandum; Feb. 15, 2007…**
  - Submit Plan By April 30, 2007 To Bring Remote Access Into Compliance With Department Policies By October 1, 2007.
  - The Plan Must Address: Use Of Two-factor Authentication.

- **FBI Response:**
  - Layered Authentication Using Two Or More Authenticators To Establish The Identity Of Sender & Receiver Of Information.

Potentials

- **Direct Users are Vetted via CJIS Identity and Authentication process**
  - **Factors based on information access requirement and home agency**
- **Federated Users are Asserted via Trust Relationships**
  - **Trust relationship parameters based on SLA**

Relevance

- **Device Protection**
  - **Authentication to Device**
  - **Data Encryption**
- **User & Device Authentication**
  - **Two-Factor Authentication to Agency**
- **Transmission Protection**
  - **Wireless Encryption**
    - **NIST SP 800-48**
- **Risk Mitigation**
  - **Security-in-Depth**

Open Discussion

- **Technologies**
- **Trends**
- **Economics**
- **?????**

Questions

George A. White

304-625-5849

gwhite3@leo.gov

BACKUP SLIDE

- **Authentication Factors**
  - **Something You Know:** Username/Password,
  - **Something You Have:** Hard Token, Soft Token, Common Access Card.
  - **Something You Are:** Fingerprints, Retinal Scan, Voice Pattern.
  - **Something You Do:** Dynamic Biometrics, E.G. Writing Signature, Keystroke Rhythm, Use Patterns.